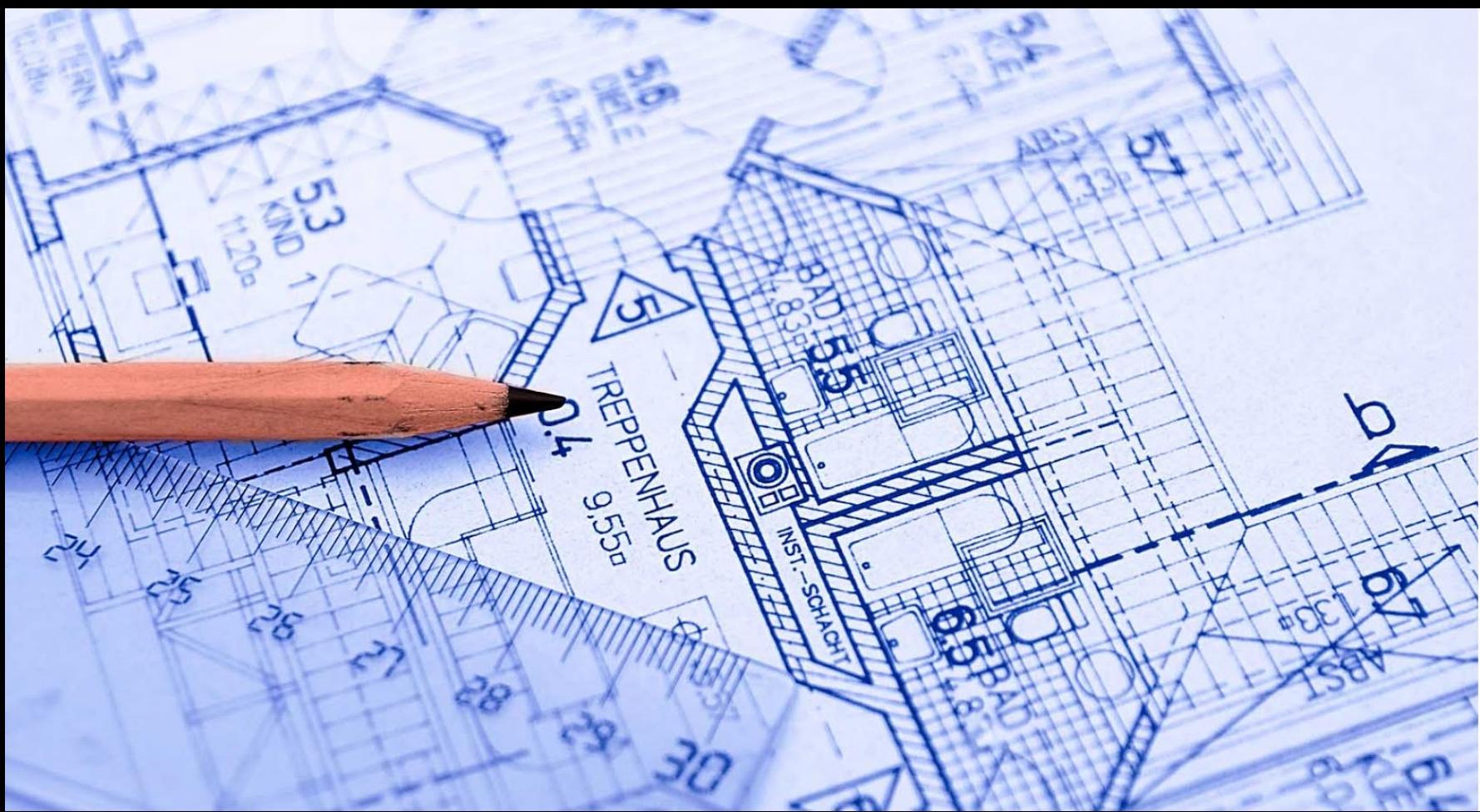


Practical Steps Taken to Reboot Vulnerability Management for Modern IT and Mature Business

Brian Canaday
IT Security Analyst/Engineer
CSAA, Insurance Group a AAA Insurer

Key Talking Points

- A Three-Phase Approach to Meeting our Vulnerability Management Goals with Qualys
- Scan Configurations & Schedule Tuning
- Cloud Agent Configuration & Testing with Application Teams





PHASE 1

Configure Scan Performance Settings Turn help tips: On | Off

Settings

Select a performance level or customize performance settings for network analysis.

Enable parallel scaling for Scanner Appliances

Overall Performance Custom ▾

1. What Scanning
2. Build Devices
3. Configure Management

Hosts to Scan in Parallel

External Scanners 30 ▾

Scanner Appliances 50 ▾

Processes to Run in Parallel (per Host)

Total Processes 10 ▾

HTTP Processes 10 ▾

Packet Delay

Packet (Burst) Delay Long ▾

Port Scanning and Host Discovery

Intensity Normal ▾

OK Cancel



PHASE 2

1. Plan and Define the Scope
2. Identify Targets
3. Identify Threats
With all data gathered
4. Test, Tune, and Verify
5. Deploy in Phases
6. Deploy in Phases

Configuring the Agent
Choose to Work
With the Agent.

Configuration Profile Edit

Turn help tips: On | Off X

Edit Mode

- General Info >
- Blackout Windows >
- Performance >**
- Assign Hosts >
- VM Scan Interval >
- PC Scan Interval >
- IOC >

Configure Agent Performance

These settings govern how an agent behaves, from how often it checks into the Qualys Cloud platform, to how often it checks the host for changes. It also includes performance settings that control CPU and network utilization.

Performance

Select one of the performance levels below. Keep the default settings **Customize** or customize them.

ON

Based On:

Set Parameters

Agent Status Interval*
Push interval in seconds to update system with Agent's status sec(900 - 7200)

Delta Upload Interval*
Interval an agent attempts to upload detected changes sec(1 - 1800)

Chunk sizes for file fragment uploads*
This is the upload block size, and combined with the above Network throttle Tx, determines network utilization KB(64 - 10240)

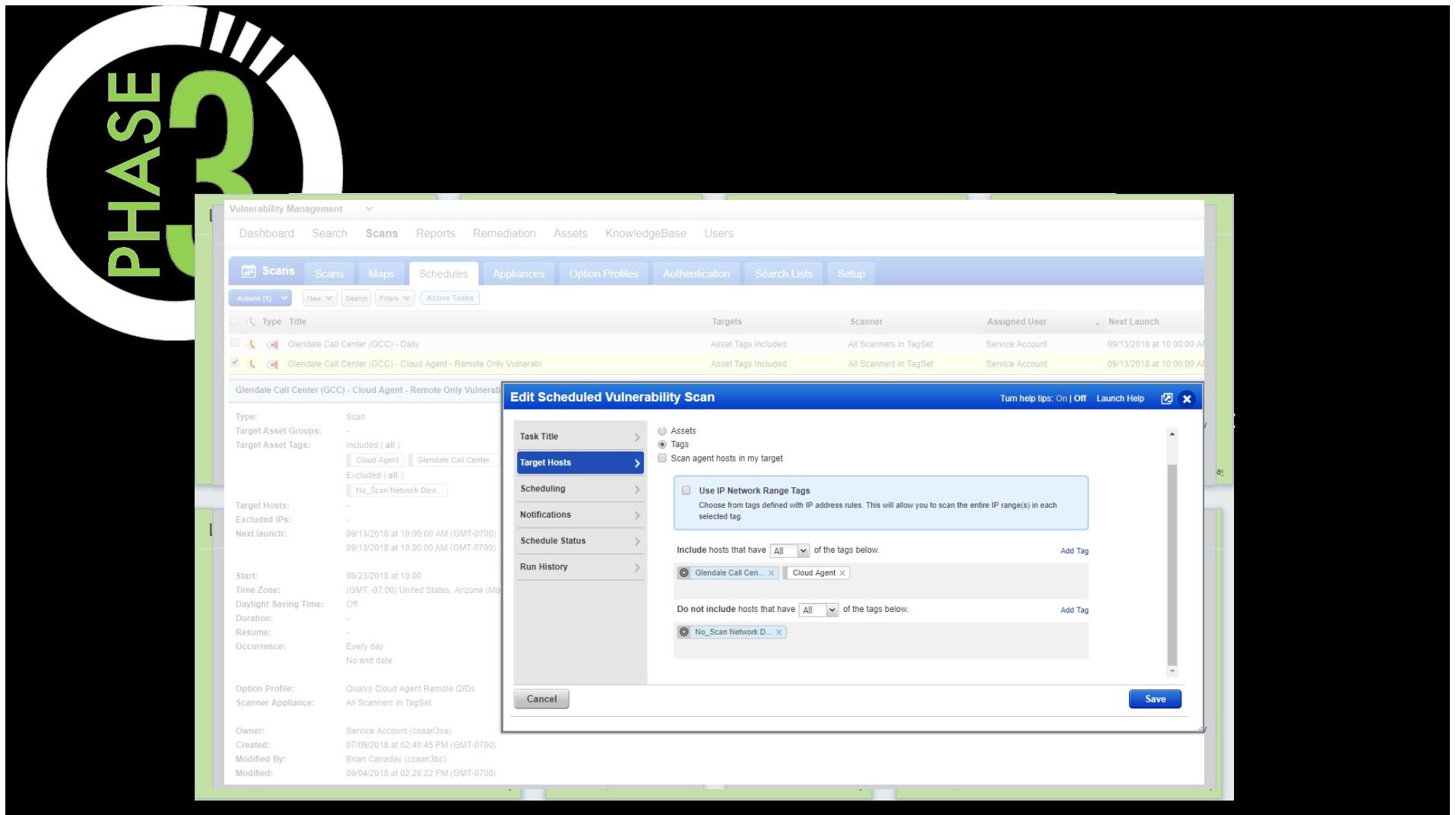
Upgrade Reattempt Interval*
Interval an agent will retry applying a new upgrade to itself sec(180 or more)

Logging level for agent*
This is the logging level for the agent.

WINDOWS SPECIFIC PARAMETERS (versions 1.5 and above)

CPU Limit*
Defines the percentage limit of the processor core(s) used by the agent. Lower percentages reduces CPU utilization at the expense of longer execution times. %(2 - 100)

Cancel **Save**



Reporting - Better Data, Better Results

- Utilizing Four With The
- 1. Applying Our
- 2. Showcasing Drills
- 3. Tracking San

Vulnerability Remediation Report

Division - Compliance

DLT Member	DLT Organization	Unique Vuln(s)	Asset Count	Critical	High	External			
		58	61	38	3	8	9	High-Crit Patch	High-Crit Config

Compliance Trend

Home > **Vulnerability Remediation Report - Organization** Home > Organization

Organization - Compliance

DLT Member	DLT Organization	Unique Vuln(s)	Asset Count	Critical	High	External			
		435	4,427	301	12	103	19	High-Crit Patch	High-Crit Config

Download

Division - Action

DLT Member
DLT Member

Organization - Action

DLT Member
DLT Member

Division - Live

DLT Member
DLT Member

Download

Vulnerability Remediation Report - Service Owner(s) Home > Organization > Service Owner

Service Owner - Compliance

DLT Member	DLT Organization	Unique Vuln(s)	Asset Count	Critical	High	Medium - Ext			
		435	4,427	301	12	103	19	High-Crit Patch	High-Crit Config

Org Leader Unique Vuln(s) Asset Count Critical Patch Critical Config High Patch High Config High-Crit Patch High-Crit Config

9	58	3	4	2	0	1	0
4	6	1	0	3	0	2	0
362	1,139	249	11	86	16	7	2
258	3,224	196	6	49	7	0	0

Application Owner Unique Vuln(s) Asset Count Critical Patch Critical Config High Patch High Config High-Crit Patch High-Crit Config

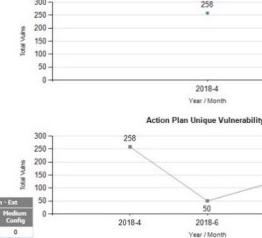
258	3,224	196	6	49	7	0	0
-----	-------	-----	---	----	---	---	---

Download

Service Owner - Action Plan

Application	Unique Vuln(s)	Asset Count	Critical	High	Medium - Ext			
		11	2	11	0			
		385	5,598	372	13	33	0	0

Every
only Items
ability to
aging the



Outcomes

- With cleaner more relevant data we can detect changes in our environment sooner
- With faster results and less impact on the systems the Qualys Cloud Agent has quickly become the one security agent our Operations Teams depend on and expect immediate remediation of any agent not reporting in
- By leveraging the API from Qualys and our CMDB we use a custom reporting solution where we rollup under the VP for each area and the leaders under them

Questions

